

TS-01-0005

科来网络分析系统 6.9
快速入门指南

技术支持部
科来软件
电话：86-28-85120922
传真：86-28-85120911
网址：http://www.colasoft.com.cn
邮件：support@colasoft.com.cn

目　录

引言

网络分析是一门非常专业的技术，需要分析者具备相当的网络知识，同时对网络分析软件使用的熟悉程度，也在很大程度决定着故障排查的效率性和准确性。但是作为初次使用网络分析软件的用户来说，他们可能会有疑问：通过网络分析软件能得到什么数据，这些数据能帮助我们做些什么，我们如何使用这些数据等等。目前流行的网络分析工具中，国外产品主要有 Sniffer，Omnipeek, Ethereal，国内产品则只有科来网络分析系统。科来网络分析系统是一个专业的网络分析软件，刚刚接触它的朋友在使用时可能存在一些疑问，不知道如何使用快速上手，下面我们就对科来网络分析系统进行简单介绍，希望能对初次使用科来网络分析系统的朋友有所帮助。

1 新建工程

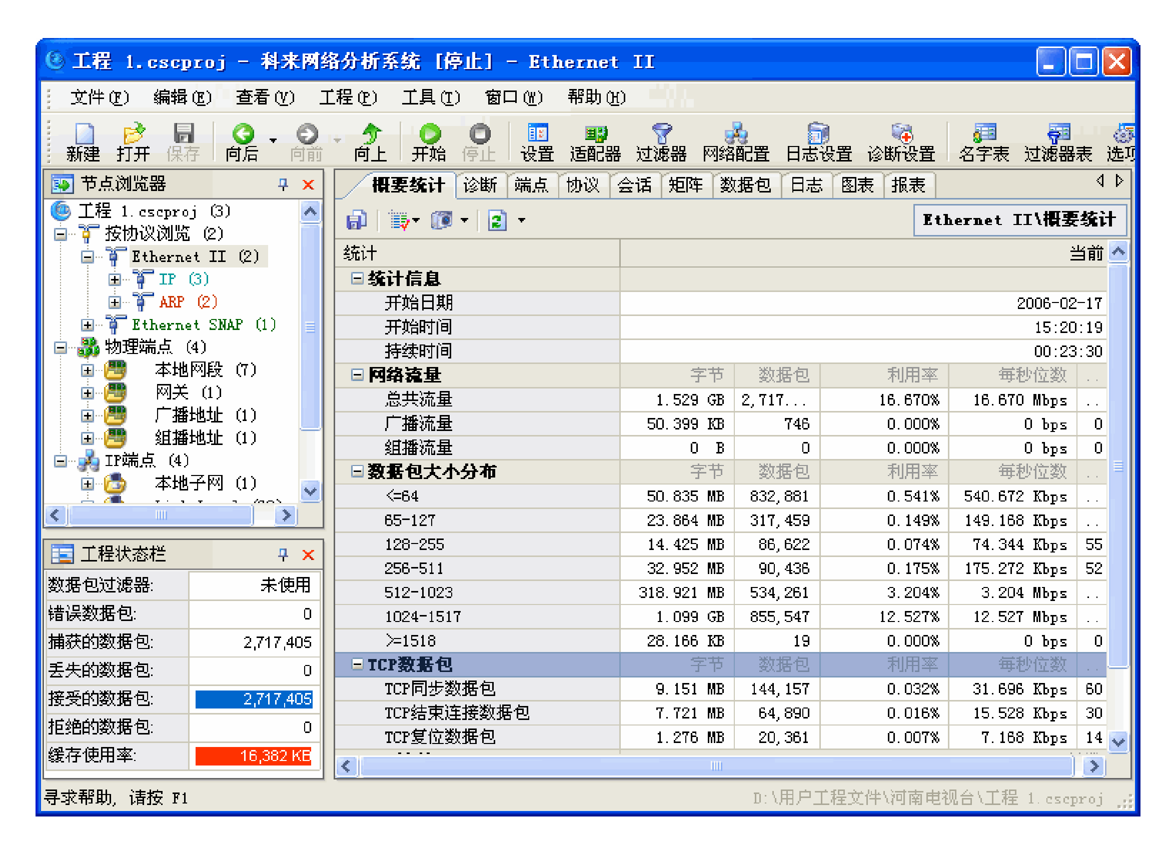
工程可以被理解为一次分析任务。捕获数据之前，用户需要创建一个新工程。系统在启动时默认创建一个新工程，用户也可以通过菜单“文件->新建”和工具栏中的“新建”进行手动创建新工程。

2 开始捕获

我们必须要对网络中的数据包进行捕获，然后才能分析整个网络，才能了解当前的网络状况。通常，用户可以从菜单中选择“工程->开始捕捉”和“停止捕捉”命令来激活科来网络分析系统或使其处于静止状态，也可以随时点击工具栏中的“开始”和“停止”图标控制工程的状态。

3 整体布局

开始捕获数据包，此时看到的是科来网络分析系统的主界面，如下图。



在主界面中我们可以发现整体主要5个部分构成：菜单、工具栏、节点浏览器、工程状态栏、主视图区。

- 菜单：提供所有的菜单命令；
- 工具栏：一些操作的快捷方式；
- 节点浏览器：按协议浏览、按物理端点浏览、按IP端点浏览；
- 工程状态栏：当前工程状态的情况；
- 主视图区：概要统计、诊断、端点、协议、会话、矩阵、数据包、日志、图表、报表。

3.1 菜单

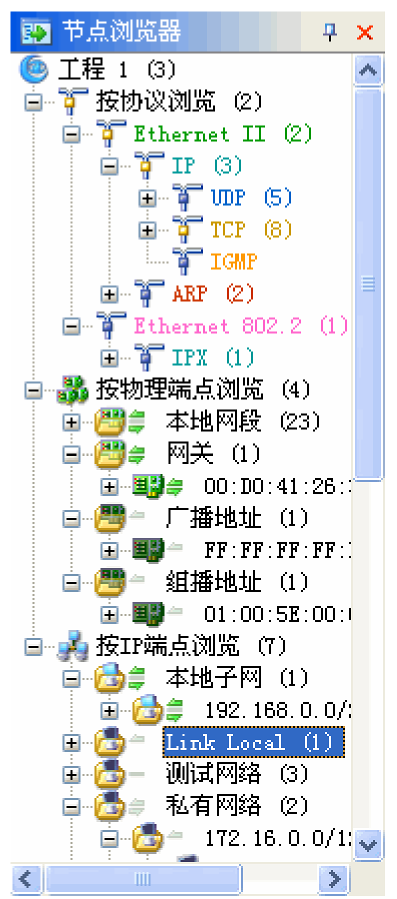
菜单提供不同的菜单命令，包括有“文件”菜单、“编辑”菜单、“视图”菜单、“工程”菜单、“工具”菜单、“窗口”菜单和“帮助”菜单。

3.2 工具栏

工具栏中的快捷按钮都可以在菜单中找到，但是这些快捷按钮给用户带来操作上的方便。用户也可以根据自己的习惯添加或删除工具栏中的快捷按钮。

3.3 节点浏览器

节点浏览器可以按协议浏览、按物理端点浏览、按IP端点浏览三类方式，它们实时的反映网络中出现的协议、主机及该主机的物理地址和IP地址，以及主机当前是否正在通讯。如下图。



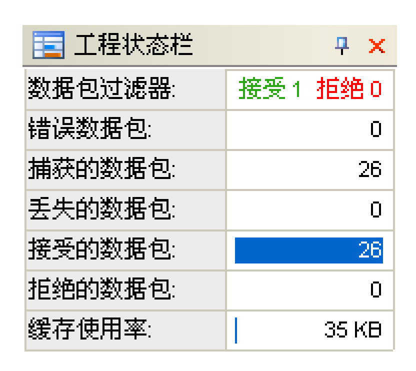
（节点浏览器）

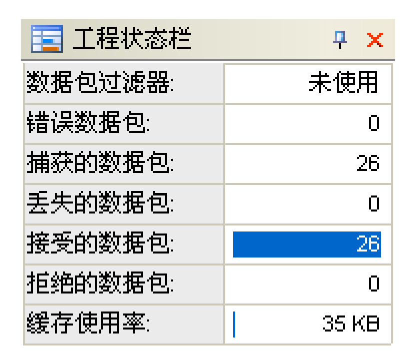


节点浏览器能让用户快速的选择需要查看的节点，并在主视图区查看相应的数据。绿色小箭头代表主机是否正在发送或者接受数据。

3.4 工程状态栏

工程状态栏实时的反映了当前工程是否使用过滤器、捕获数据包的详细情况、以及缓存使用情况。如图。





如果设置了过滤器，在工程状态栏中的“数据包过滤器”为“接受1 拒绝0”；如果未设置过滤器则显示为“未使用”。

3.5 主视图区

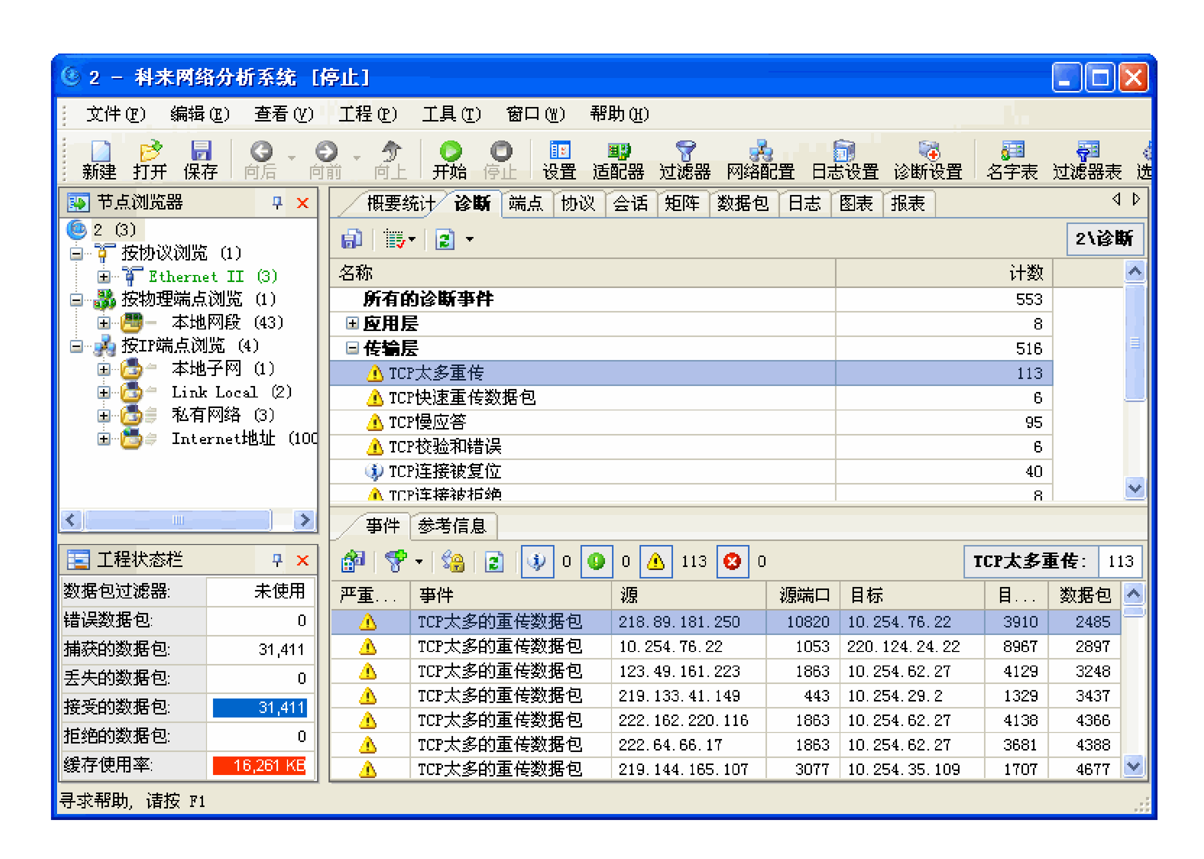
主视图区在系统窗口的右边，包括概要统计视图、端点视图、协议视图、数据包解码视图、会话视图、日志视图、图表视图、报表视图。点击相应的视图标签，则可以查看相应的网络分析数据。主视图区分别由10个视图部分组成：

- 概要统计



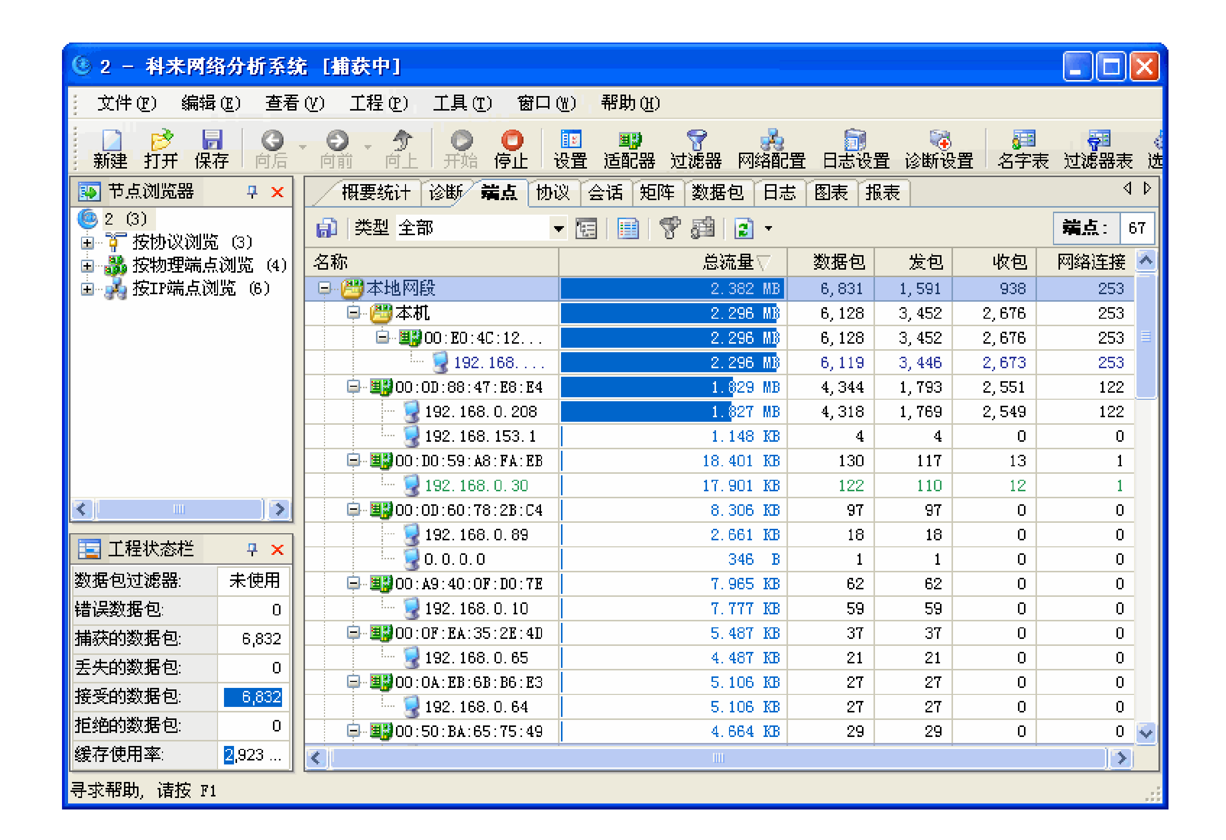
该视图中可以看到捕获数据的时间，网络流量，数据包大小分布等等信息。如果网络中流量很大时，可以使用快照功能对不同时刻的流量进行对比分析。

- 诊断



系统将捕获的数据包进行智能的分析，在诊断视图中进行专家诊断提示，帮助用户快速查找出各种异常情况的源和目的主机。诊断视图中带有诊断事件参考信息，将事件可能出现的原因及解决方法提示给用户。

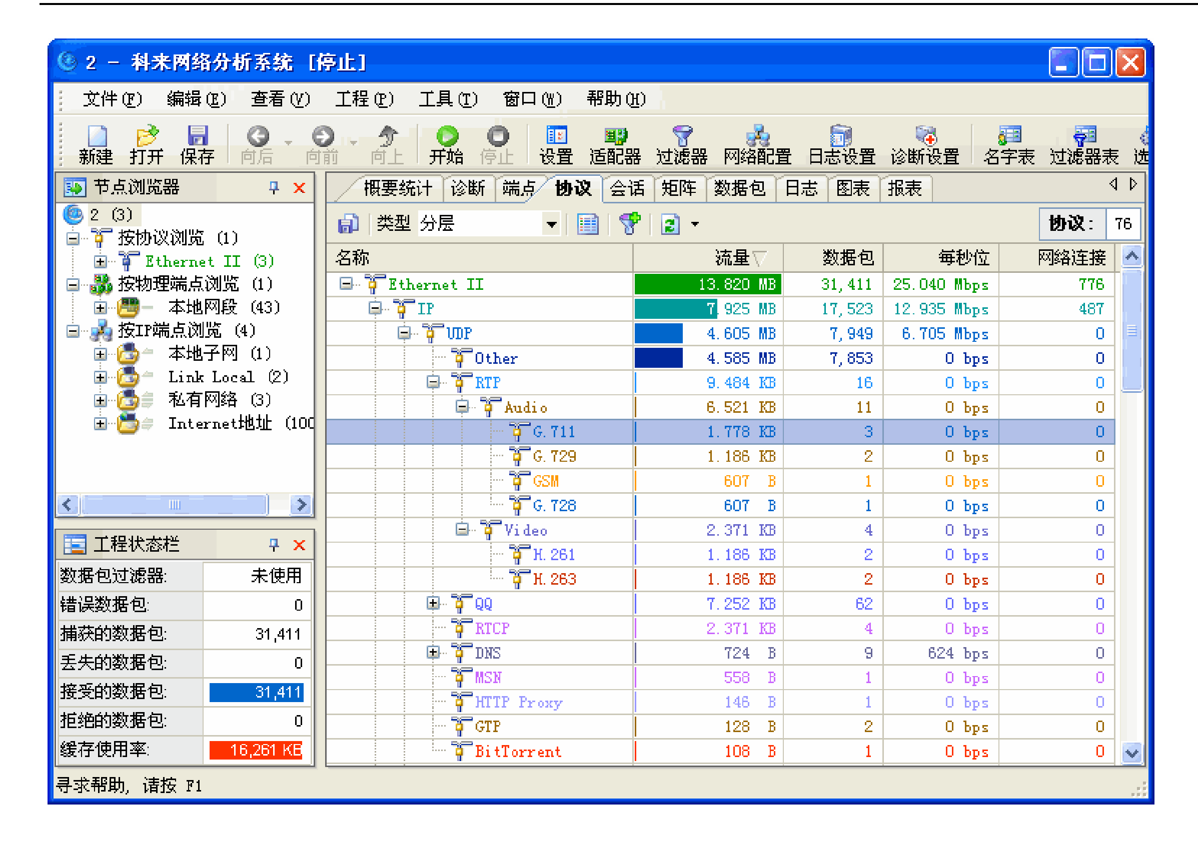
- 端点



端点视图可以按物理端点和 IP 端点两种类型查看，用户可以快速找定位通讯量最大的 IP 端点和物理端点，可以清楚地得出当前网络中所有主机（包括一个网段、一个物理 MAC 地址、一个 IP）的具体流量占用情况，如总流量最大的主机、发送流量最大的主机、接收流量最大的主机、收发数据包数最多的主机、发送数据包最多的主机、接收数据包最多的主机、内部流量、以及广播流量最大的主机等信息。

通过这些信息，我们可以确定网络中是否广播/组播风暴，并帮助用户排查网络速度慢、网络时断时续、蠕虫病毒攻击、DOS 攻击、以及用户无法上网等网络故障。

- 协议

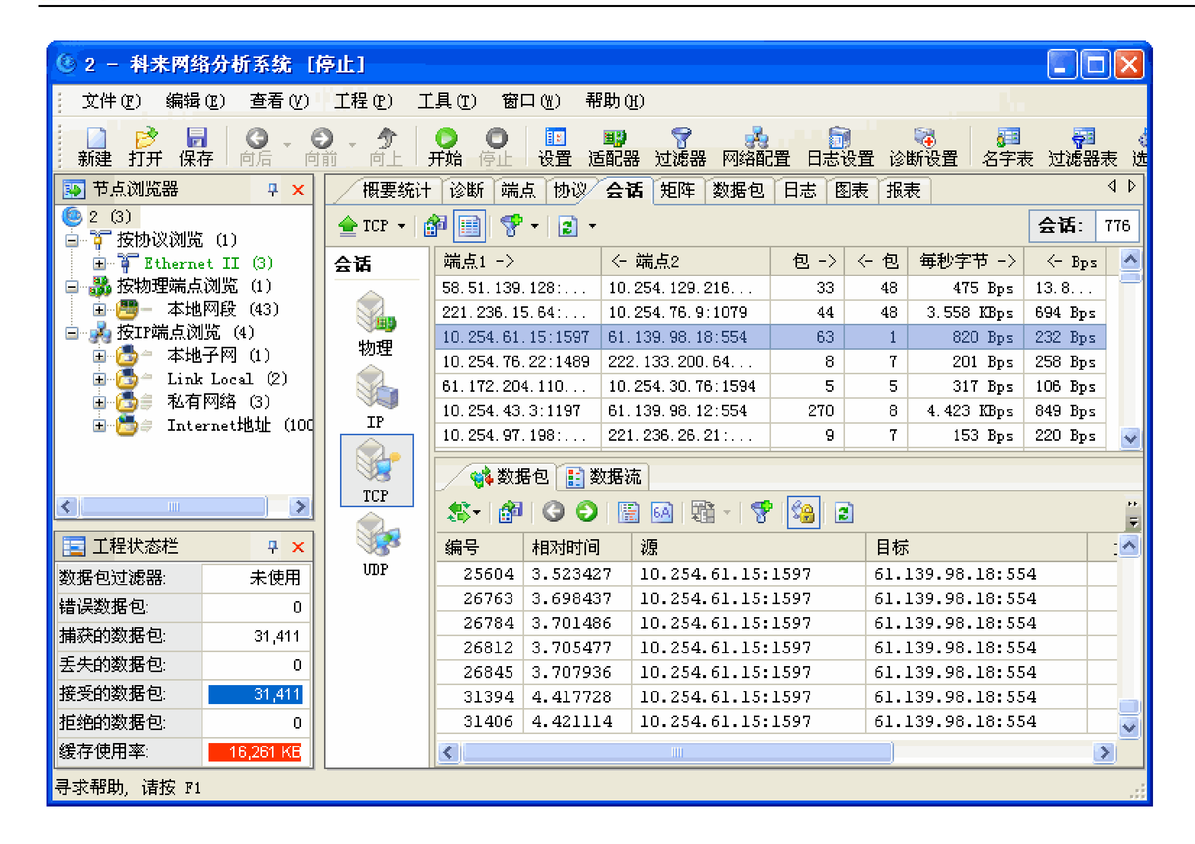


协议视图全局的协议统计，它提供每个网络端点下的协议统计数据，遵循 OSI 七层协议分析，根据实际的网络协议封装顺序，层次化的展现给用户，协议之间有不同色彩，方便用户查看。

协议视图有两种显示类型：以太网和 IP。用户可以选择两个类型来查看协议分布情况，它们起一个过滤作用。如果用户选择以太网类型，那么系统就是按照数据链路层协议来过滤器统计；同理，用户选择 IP 类型，那么系统就是按照 IP 协议来过滤统计。

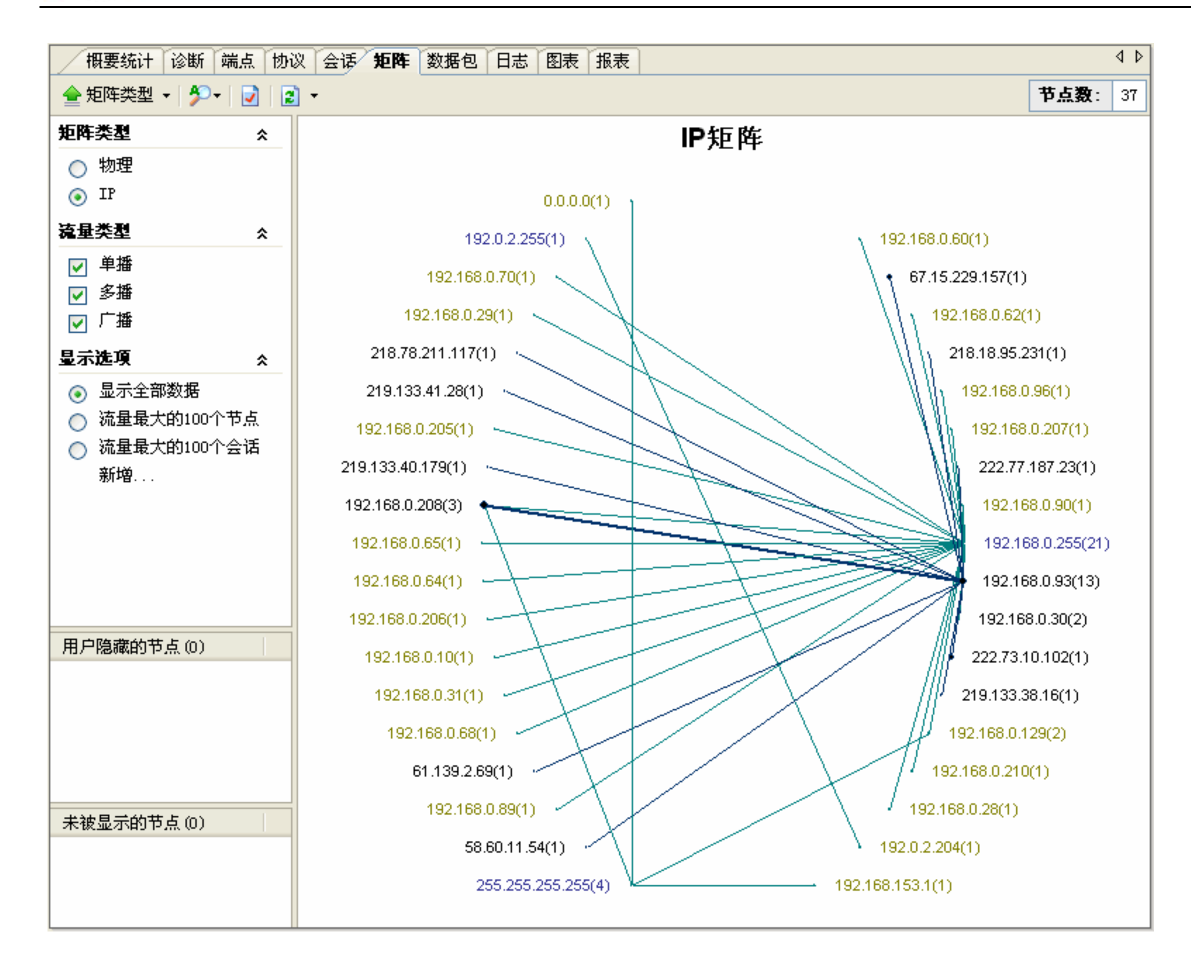
通过协议视图对各协议占用流量及百分比的统计，用户可以得出当前网络中占用流量最多的协议，即当前网络中占用流量最多的服务类型；并帮助用户排查网络速度慢、邮件蠕虫病毒攻击、网络时断时续以及用户无法上网等网络故障。

- 会话



会话视图提供物理地址、IP 地址、TCP 连接、UDP 会话用来显示网络中的会话信息。并在下方的子窗口中显示当前选定会话的数据包等信息。通过查看每条会话，我们可以统计其源地址、目标地址、该会话收发的数据包及这些数据包的大小等信息。我们可以通过这些信息确定出当前网络中某个会话的通讯情况。特别在 TCP 会话中，系统将 TCP 数据流进行重组，用户可通过 TCP 数据流窗口查看。

- 矩阵



矩阵视图用于实时显示网络通讯的节点和会话信息。用户可以选择不同的类型来查看矩阵视图，矩阵类型有物理地址和IP地址两种，同时只能选择查看一种类型的矩阵，系统默认选中的是IP。

- ✓ **物理地址：**根据物理地址（MAC 地址）节点显示矩阵内容；
- ✓ **IP 地址：**根据 IP 地址节点显示矩阵内容。

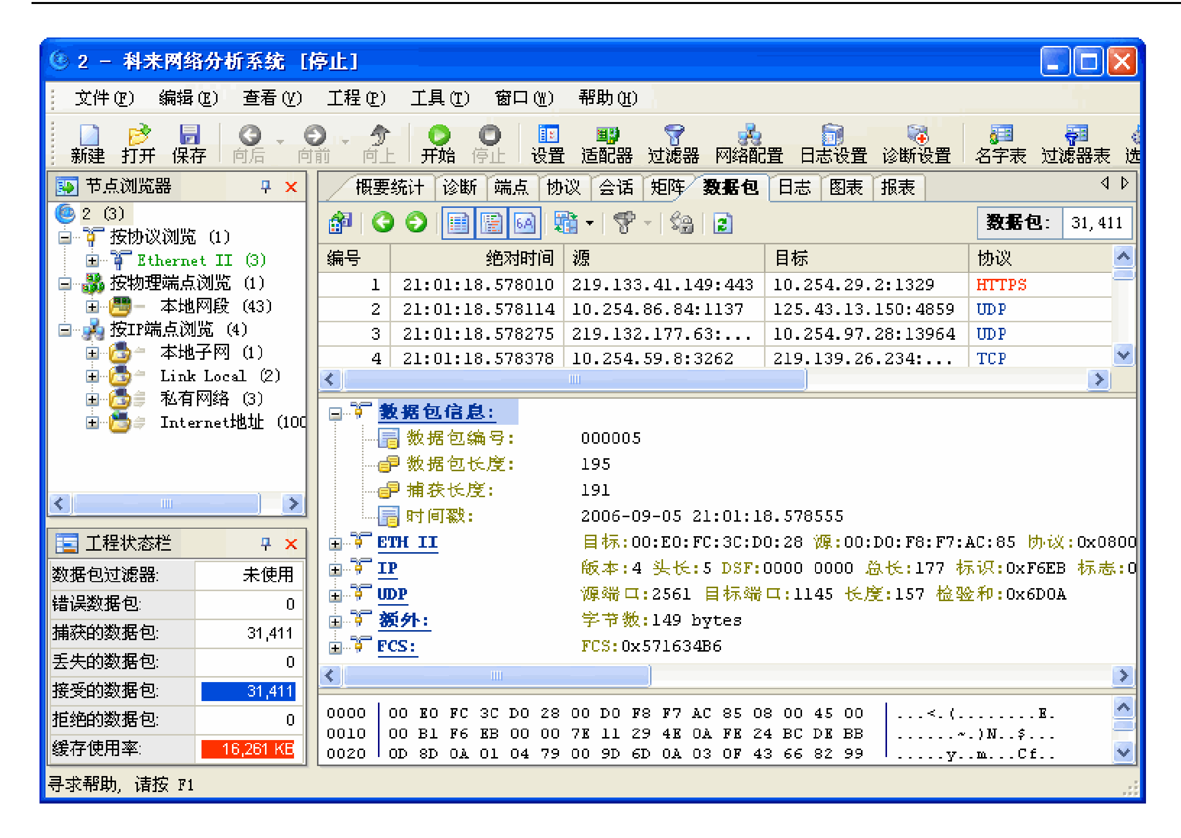
流量类型有单播、多播和广播三种，可以同时选择查看一种或多种类型的流量，系统默认将三种流量全部选中。

- ✓ **单播：**目标地址和源地址都是单播地址的流量，称为单播流量，选中单播后，右边的矩阵内容显示区会显示网络中单播流量的矩阵信息；
- ✓ **多播：**目标地址或源地址是多播地址的流量，称为多播流量，有时也称为组播流量，选中多播后，右边的矩阵内容显示区会显示网络中多播流量的矩阵信息；
- ✓ **广播：**目标地址或源地址是广播地址的流量，称为广播流量，选中广播后，右边的矩阵内容显示区会显示网络中广播流量的矩阵信息。

显示类型默认有“显示全部数据”、“流量最大的 100 个节点”、“流量最大的 100 条会话”、 三个选项和一个“新增...”功能，选项类型之间是单选。

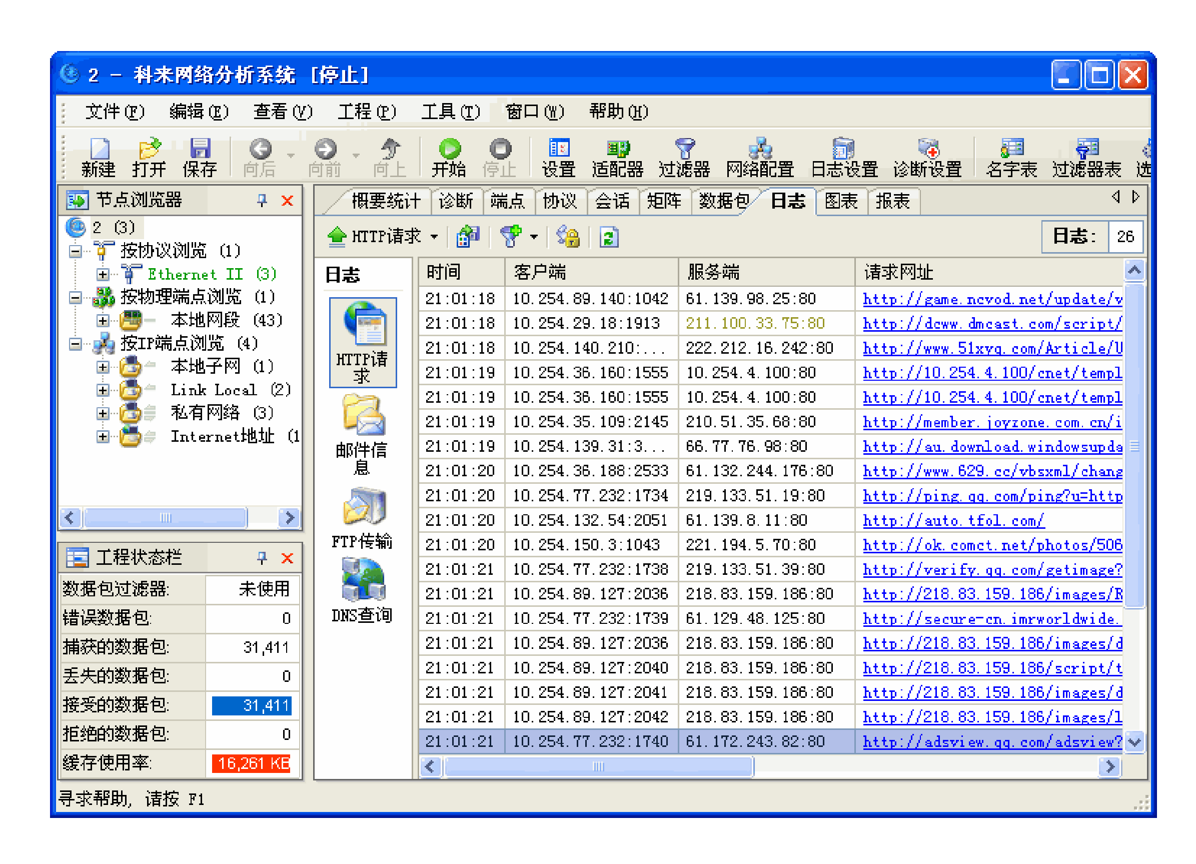
- ✓ **显示全部数据：**显示符合矩阵类型、流量类型设定的所有矩阵信息；
- ✓ **流量最大的 100 个节点：**显示符合矩阵类型、流量类型设定的流量最大的 100 个节点的矩阵信息；
- ✓ **流量最大的 100 条会话：**显示符合矩阵类型、流量类型设定的流量最大的 100 条会话的矩阵信息；
- ✓ **New：**添加自定义的显示过滤条件，单击后弹出窗口，用户可根据自己的需要进行设定。

- **数据包**



在数据包视图，我们可以看到详细的解码信息：概要解码，字段解码，十六制解码。概要解码是自动进行，用户也可以选择概要解码的协议层，帮助用户快速定位可疑的网络数据包，使用解码列也可以帮助用户进行数据包之间的解码对比。用户还可以选择单个数据包进行详细解码，详细解码字段可以和数据包原始数据互动，即便是精心伪造的网络攻击、欺骗数据包在这种模式下也无所遁形。

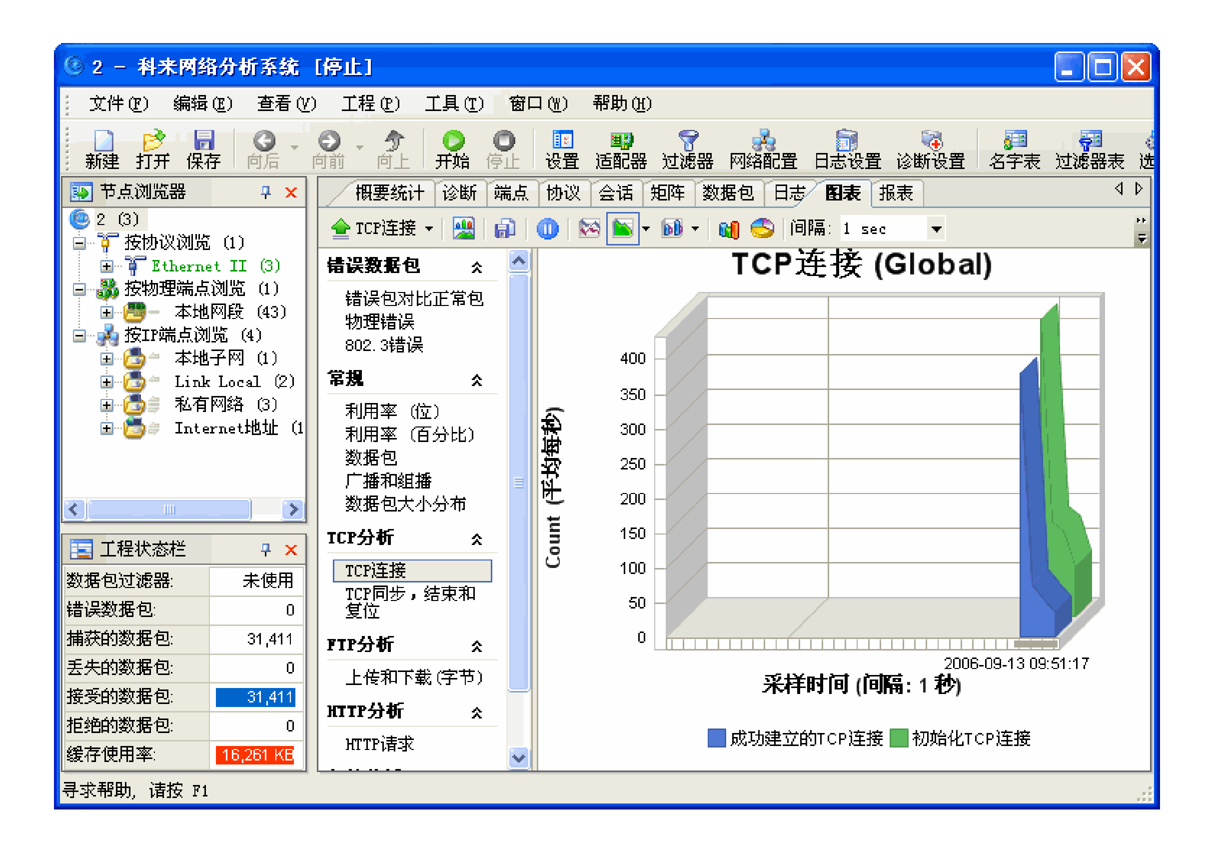
- 日志



日志视图记录网络中用户的高级网络运用，包括HTTP请求（网页浏览），邮件信息（使用SMTP/POP3

协议的邮件收发），FTP传输（使用FTP协议的数据上传下载） 以及DNS分析（查看用户的DNS请求和响应情况）。用户可根据需要将这些日志信息保存到硬盘以备查阅。

- 图表



图表功能为用户提供2D或者3D的时间趋势图和数据比较图，可以选择折线图、柱状图、面积图、饼图等多种形式，除了全局图表，也支持每个协议和网络端点的图表数据采集显示。

- 报表



报表视图将统计分析的结果以报表的形式输出，用户根据报表的数据便可对当前的网络情况有一个全面的掌握。

报表视图中，实时的统计数据并将通讯情况在报表视图中产生报表信息。报表包含了统计分析的主要内容，包括概要统计的全部内容、协议使用统计明细、流量最大的前10个IP地址、前10个MAC地址以及各种图形统计结果。默认没有开启图形统计，用户可以在选项中选择性的添加。

4 工程设置

启动科来网络分析系统，点击“立即开始采集”按钮，默认会打开工程设置窗口（可以在选项中取消）。用户可以根据需要对工程设置中的常规、网络适配器、过滤器、网络配置、日志设置、诊断设置选项进行自定义设置。

4.1 常规

工程设置

常规 网络适配器 过滤器 网络配置 日志设置 诊断设置

数据包缓存大小: 16384 千字节

当缓存装满时: 丢弃最早的数据包 (循环缓存)

自动保存数据包文件

限制每个数据包为 60 字节

单个文件

多个分割文件

保存到文件夹:

基本文件名:

文件分割间隔: 1 天

保留所有文件 保留最近的 1 个文件

数据统计设置

启用每个网络端点的详细协议统计。 启用每个协议的IP和物理会话统计。

启用详细的数据包大小统计。 按国家对IP地址分组。

启用自定义端口

当开始捕获数据时总是显示工程设置.

保存为默认设置 OK Cancel Help

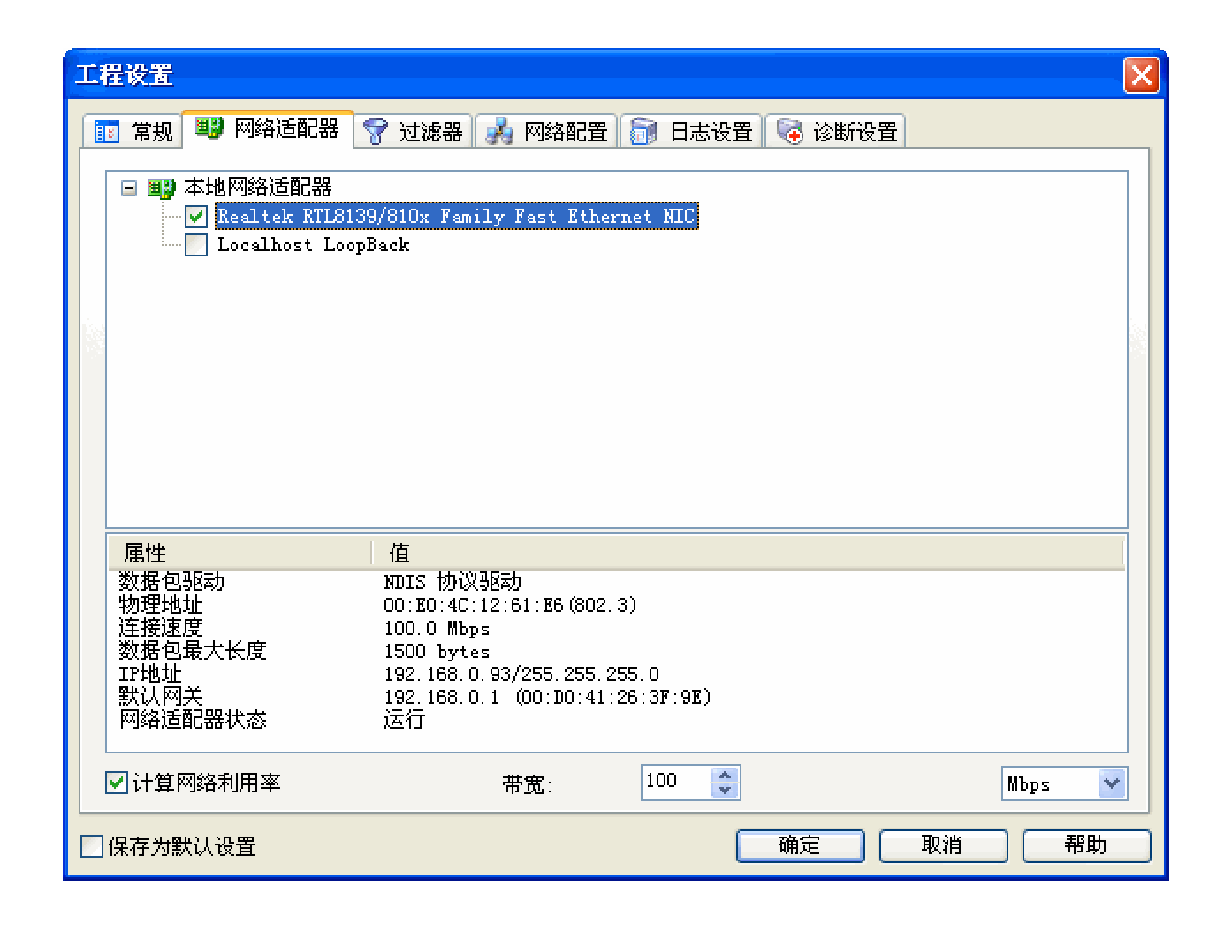
在常规选项中，主要是数据包缓存设置（默认 16M）、缓存器装满时的处理方法（默认是第一种循环缓存）。

用户也可以将采集到的数据在分析这前进行保存，可以将原始数据信息保存下来供以后分析；保存的数据包文件可以是单个的文件，也可以按照时间或大小保存为多个文件。

数据包截断功能：用户可以设置限制值 X，以保证数据被保存为文件时仅保留前 X 个字节。

在大型网络中，启用按国家对IP地址分组会占用大量内存,启用每个会话的详细协议统计会降低分析效率，默认没有启用。

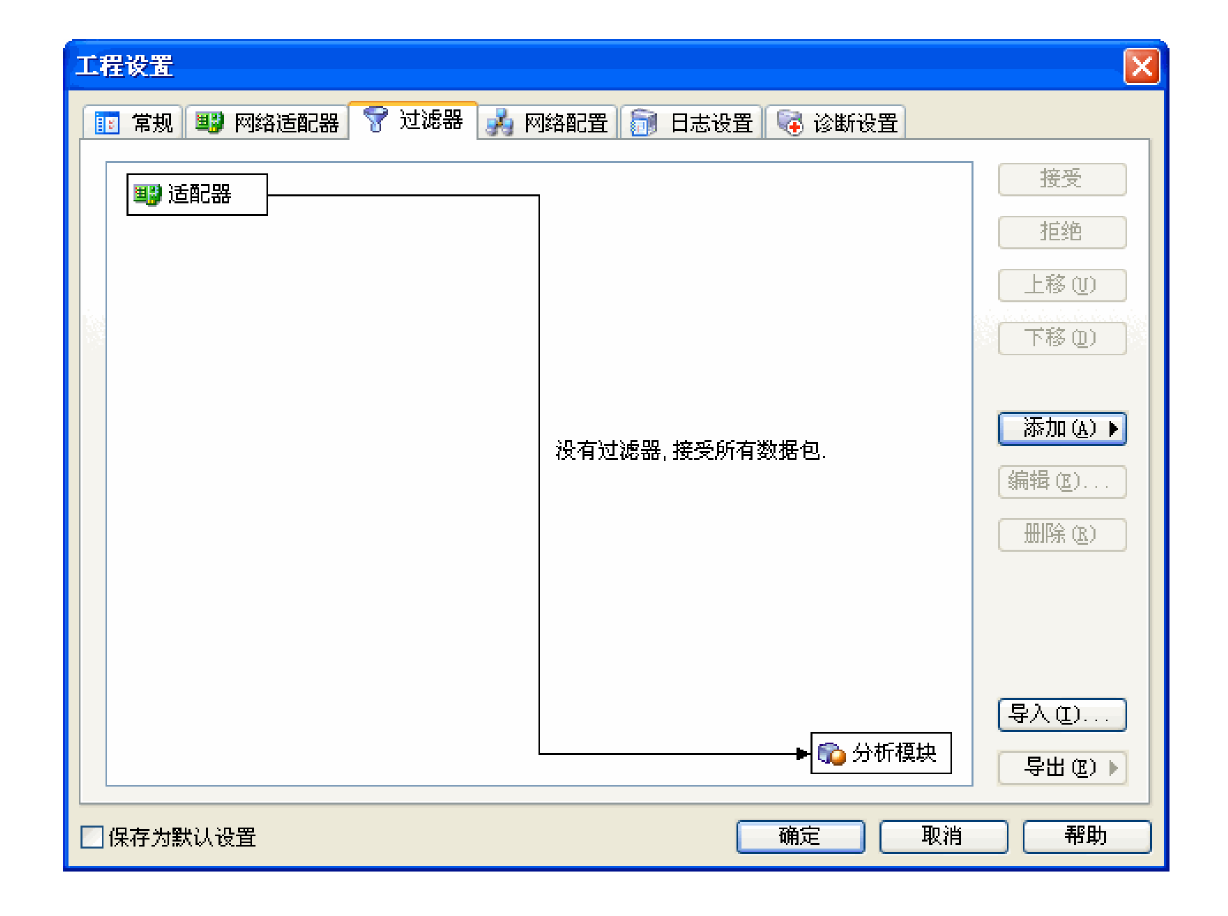
4.2 网络适配器



在网络适配器中，需要选择捕获的网卡，主要是选择数据采集方式。科来网络分析系统支持以太网、拨号上网、本地环回方式的数据采集，并且也支持多网卡采集，用户可以选择一个网卡或多个网卡来捕获数据包。

科来网络分析系统也能自动识别网卡的传输速度，默认以网卡的速度为网络带宽，用户也可以根据实际情况改变此值。如网卡虽然为 1000M，但内网的网线却是 100M，为了使统计更附合实际，可将带宽改为 100M。

4.3 过滤器



设置过滤器是我们改变捕获数据范围的重要手段。通过过滤器，我们可以只捕获所需的数据包，把重要的数据分离出来。这样用户就可以只关注存在网络故障或网络攻击的数据信息，而不用在大量的数据中逐个寻找。

用户可在工程设置中来定义过滤器设置。科来网络分析系统提供了一个默认的过滤器列表。这些过滤器都是以协议为条件的过滤器，每个过滤器都可以使用“接收”和“排除”来指定其过滤条件，也可以随意组合其中的过滤器来制定数据包的捕获范围。

用户也可自定义过滤条件来设定过滤器，按照直观性，就分为简单过滤器和高级过滤器。

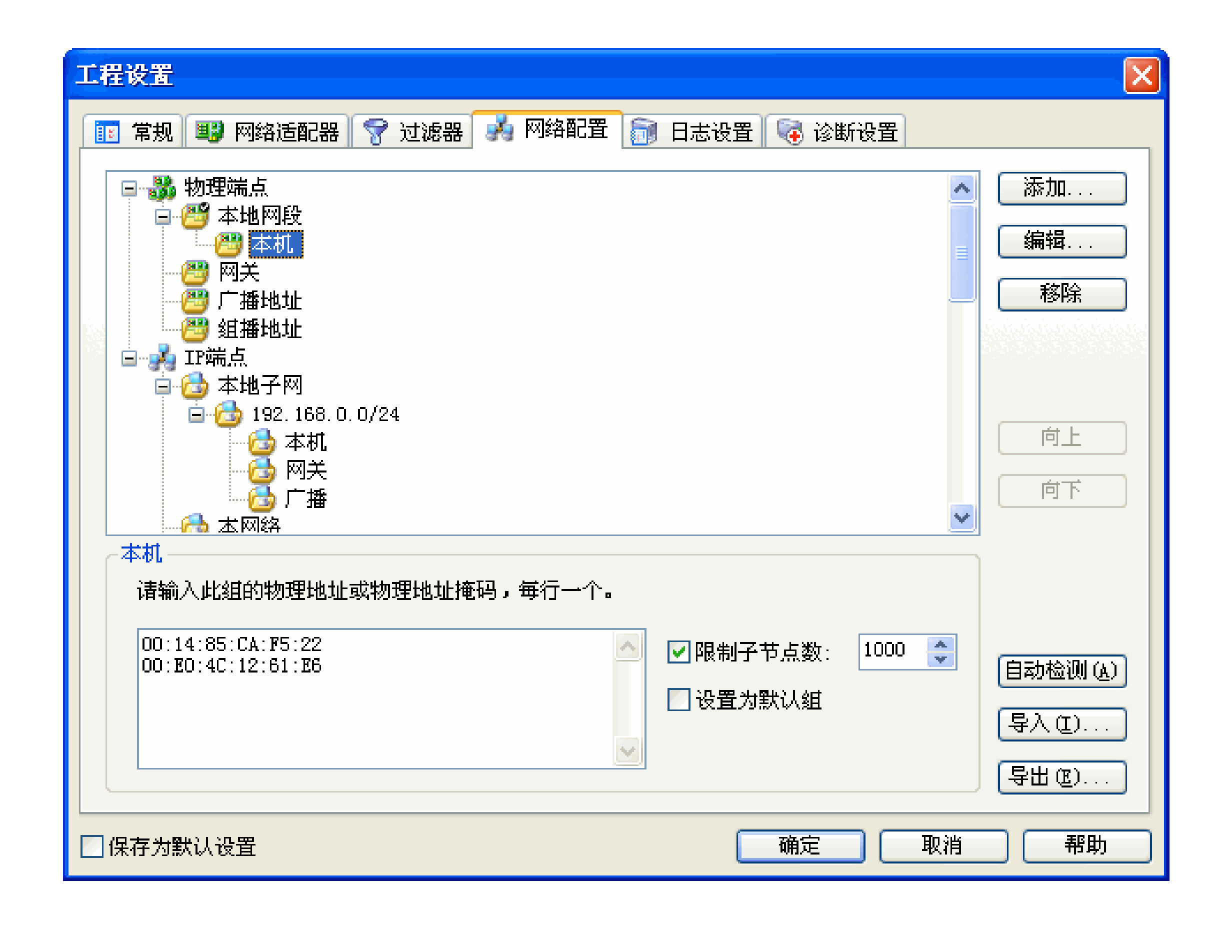
- **简单过滤器**

简单过滤可以让我们使用常用的筛选条件，如 IP 地址、MAC 地址、端口、协议等。在设置 IP 地址、MAC 地址、端口这些条件时，可以选择数据包传输的方向。这样可以很精确的进行筛选数据。而设定协议条件时，可以选择一个或多个协议进行筛选。简单过滤中的筛选条件可以任意组合，并且为了查看方便，可指定协议的颜色以区别其它协议。

- **高级过滤器**

高级过滤增加了“数据包值”筛选、“数据包大小”筛选和“数据包模式配置”筛选条件，并提供多种逻辑关系来组合各种条件。而且高级过滤设置提供一个非常直观的过滤关系图，图中将展示设定的过滤条件的逻辑关系，通过网卡到主机的过达路径，便可以很轻易看出过滤器的条件关系。

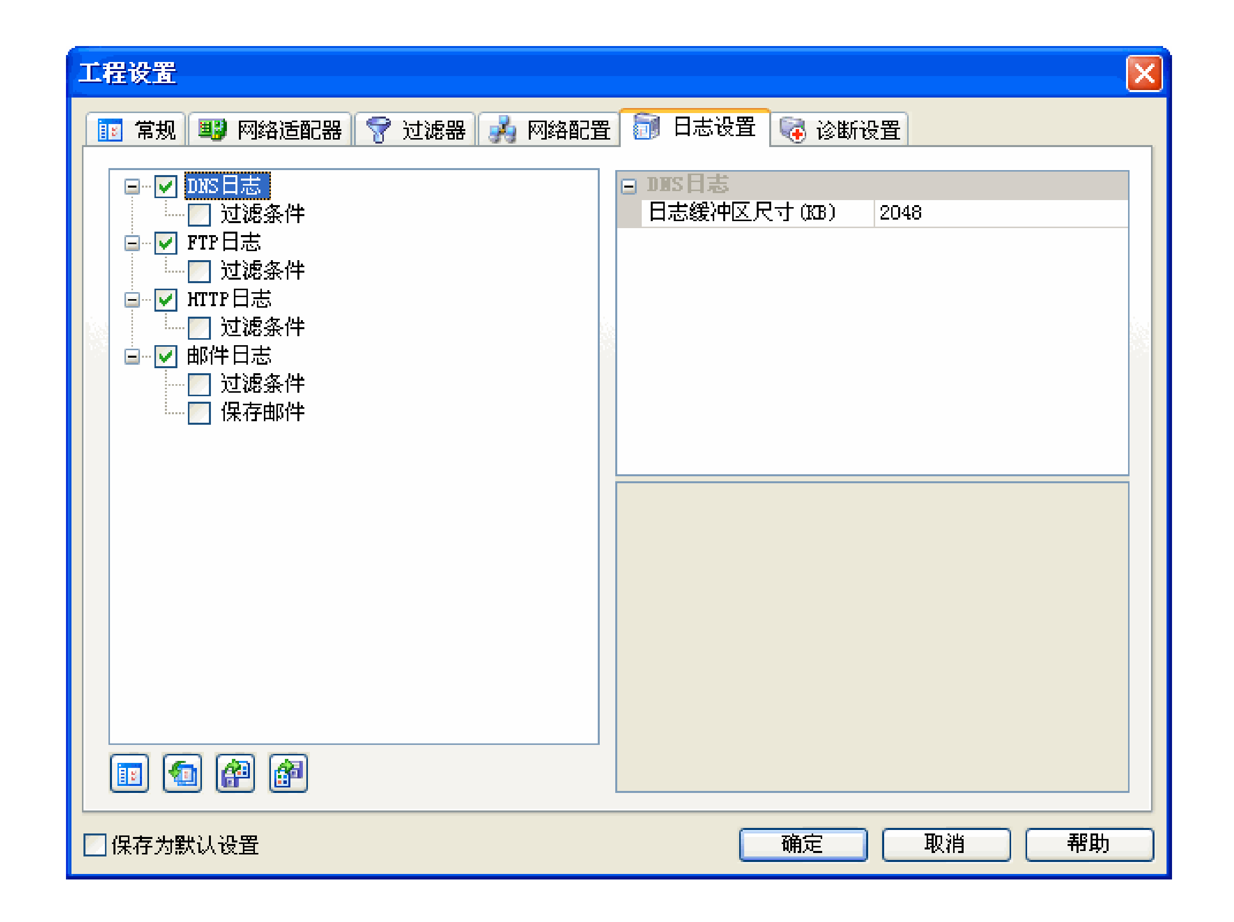
4.4 网络配置



网络配置主要是自定义节点浏览器中 IP 节点和 MAC 节点。用户可以根据需要添加、删除来规划自己的网络结构。例如，为了便于管理，可以把不同网段分成不同 IP 组里，也可以按照部门建立不同的 IP 组。

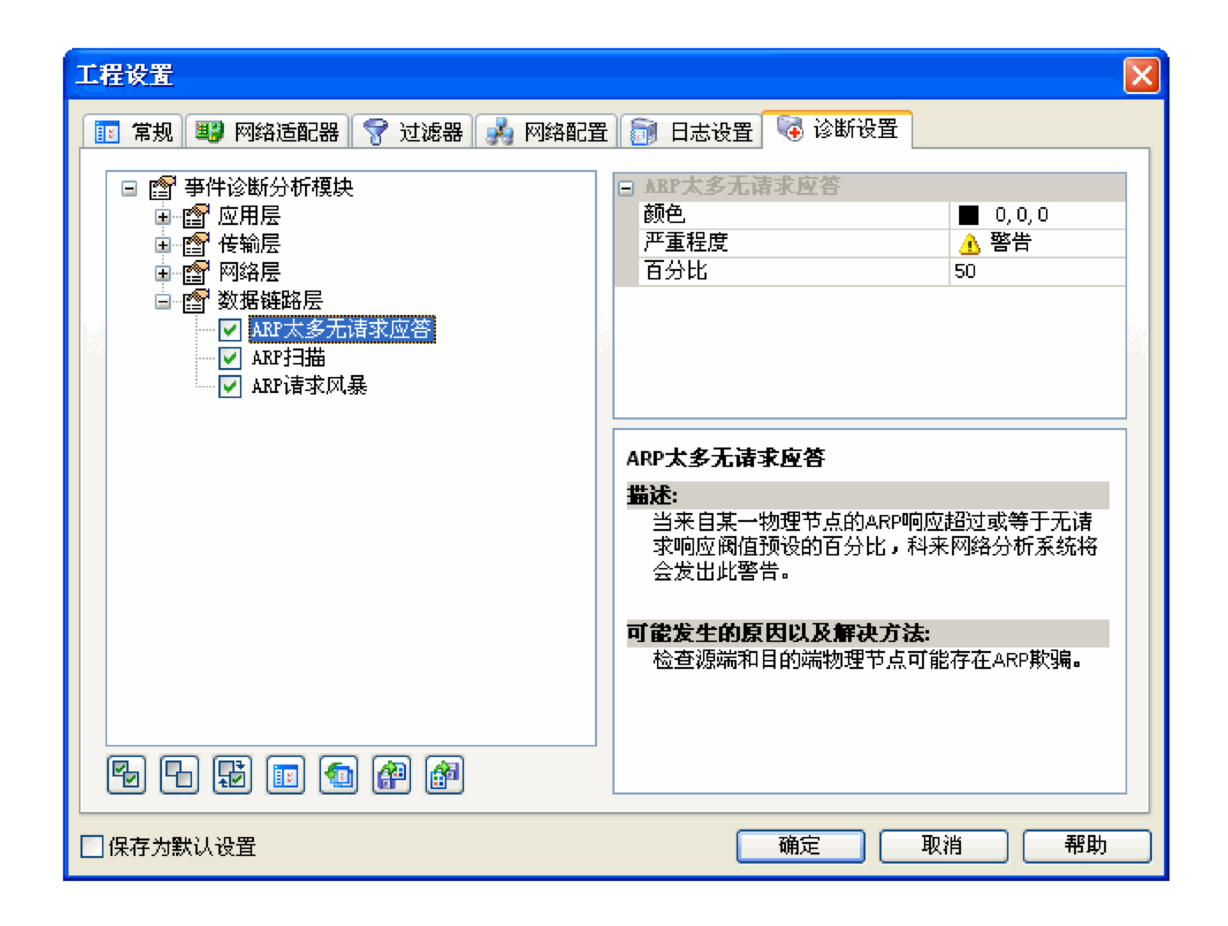
科来网络分析系统有一个默认的配置，点击自动检测，系统将对网络进行自动扫描，将 IP 节点和 MAC 节点自己检测出来。最后在节点浏览器中体现出来。

4.5 日志设置



日志视图记录网络中用户的高级网络运用，包括 HTTP 请求（网页浏览），邮件信息（通过 SMTP/POP3 进行的邮件收发）、FTP 传输（通过 FTP 进行的数据上传下载） 和 DNS 分析（域名解析），并可根据用户的需要将这些日志信息保存到硬盘以备查阅。默认时日志过滤器都没启用。

4.6 诊断设置



诊断设置中，包含了系统内置的所有诊断事件，用户可以根据自身的网络情况，更改诊断事件的设置，如颜色、严重程度、阈值等。默认时，各个诊断都是全部启用的，如果用户不想启用诊断的事件，用户也可以在列表中，取消该事件的诊断应用。对于诊断设置中的配置，我们可以通过导入导出来与其他人员共享；如果设置混乱了，用户也可以采取恢复默认值。

以上简单描述工程设置的相关内容。工程设置可以根据用户自己的情况进行设置，或者使用以前的默认设置，完成这些设置以后就可以开始捕获数据了。

5 数据管理

科来网络分析系统可以对工程文件以及工程中的数据进行有效管理。

5.1 工程文件

保存工程

工程保存有利于以后对数据进行再次查看。用户可以通过保存工程文件来保存当前的分析结果，同时也能保存工程设置中的所有选项。用户可以从菜单中选择“文件->保存”或者从工具栏中的“保存”按钮执行操作。工程的格式为“.cscproj”。

保存为模板

用户可以将工程保存为模板，在以后使用的时候可以导入模板，这样用户就可以使用当前模板中的设置。用户可以从菜单中选择“文件->另存为模板”。模板的格式为“.csctemp”。

导出工程

科来网络分析系统也可以导入和导出工程。这里的导出工程和保存工程是有区别的。导出工程只保存工程中所有的数据包，而保存工程则包含有所有数据包及工程中设置的所有选项。

5.2 数据包

科来网络分析系统也支持对工程中单个和多个数据包以特定的格式保存，同时也可以导入多个数据包文件。

- 导出数据包

用户可以将数据内容导出到一个特定格式的文件。科来网络分析系统除了支持基本的*.txt、*.csv、*.html 格式的文件，也支持通用的 Sniffer、Etherpeek 等工具的文件格式。

用户也可以设置需要导出的数据内容，如下图所示：



- ✓ *.txt (文本文件)
- ✓ *.csv (csv 文件) ；
- ✓ *.html (html 文件) ；
- ✓ *.cscpkt (科来网络分析系统数据包文件);
- ✓ *.cap (Sniffer 数据包文件) ；
- ✓ *.pkt (EtherPeek/AiroPeek 数据包文件);
- ✓ *.rawpkt (Raw 数据包文件) ；
- ✓ *.cap (Libpcap Tcpdump,Ethereal,等通用数据包文件) ；
- ✓ *.dmp(Libpcap Tcpdump,Ethereal,等通用数据包文件);
- ✓ *.cap (Microsoft Network Monitor 2.x) ；

- 导入数据包

科来网络分析系统支持多种通用数据包格式的导入，你可以导入数据包文件到工程中进行分析。支持导入的文件类型如下图所示：



- ✓ *.cscpkt (科来网络分析系统数据包文件) ；
- ✓ *.cpf (科来网络分析系统 4.0 数据包文件) ；
- ✓ *.cap (Network Associates Sniffer 数据包文件) ；
- ✓ *.pkt (EtherPeek/TokenPeek/AiroPeek 数据包文件) ；
- ✓ *.pkt (Etherpeek Packet File V7) ；
- ✓ *.pkt (Omnipeek Packet File V9) ；
- ✓ *.rawpkt (Raw 数据包文件) ；
- ✓ *.cap (Libpcap Tcpdump,Ethereal,等通用数据包文件)；
- ✓ *.dmp(Libpcap Tcpdump,Ethereal,等通用数据包文件)；
- ✓ *.cap (Microsoft Network Monitor 2.x) ；